SECTION 3 INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY (IT)

Critical success over the next five years can be defined as creating a common operating environment that fully leverages IT products and services throughout the Corps. For purposes of managing IT projects and services, the Command FY 03 Functional Area Assessment (FAA) metrics serve as excellent benchmarks. The specific metrics include: Achieve a mission-to-support ratio of 60/40%; reduce regional overhead by 10%; reduce process time by 30%; reduce labor costs by 10%.

Assumptions:

- The focus of all business transactions and management will be regionally focused by the year 2012.
- Although a critical business enabler, Information Technology/Information Management (IT/IM) functions are not a USACE core competency.
- There are IT/IM functions that are inherently governmental in nature and there are IT services that lend themselves to outsourcing.
- The economies of scale and efficiencies gained by regionalizing IT/IM functions can be substantiated.
- There are tools that can effectively provision and manage IT services from regional or centralized locations.
- The USACE will experience a large number of retirements in the CP34 Career Program within the next 5 years.
- IT/IM services will continue to be viewed as G&A/overhead.

This Command guidance contributes to alignment of IT with our business processes to ensure interoperability, technology and e-government innovation, systems modernization, information security, and capture of explicit and tacit organizational knowledge. Command guidance is presented within the following goal areas of the USACE Information Resources Management (IRM) Strategic Plan (draft):

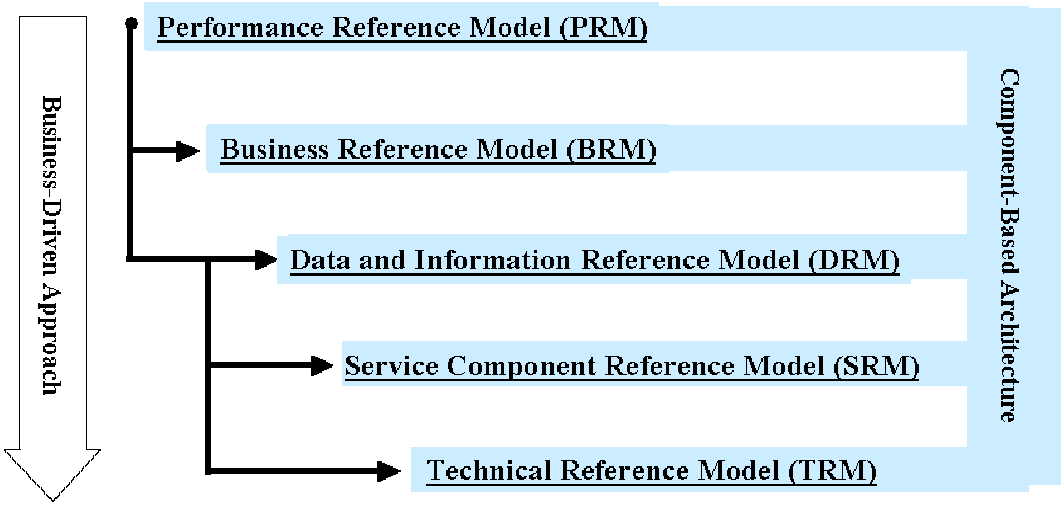
GOAL 1	IT INFRASTRUCTURE
GOAL 2	TECHNOLOGY INSERTION
GOAL 3	INFORMATION ASSURANCE (IA)
GOAL 4	IT INVESTMENT PORTFOLIO MANAGEMENT
GOAL 5	E-GOVERNMENT

Goal 1: IT Infrastructure. Provide an IT infrastructure that will ensure information superiority and connectivity throughout USACE.

Key Outcome Measures: Reduced unit cost to customers; improved network performance; IT architecture and investment alignment; web server and support consolidation on both a regional and enterprise-wide basis; reduced total cost of ownership.

Corps Enterprise Architecture (CeA). CeA provides USACE-specific building blocks to align IT investments with USACE business needs, while at the same time, supporting the Federal Enterprise Architecture Framework (FEAF) and the DoD's Command, Control, Communications, Computers, Information, Surveillance & Reconnaissance (C4ISR) Framework. The diagram below identifies the top-level models of the Federal Enterprise Architecture. In FY 04, all organizational levels will begin making IT investments based on the CeA Transition Plan. More information on CeA will be published at https://cea.hq.usace.army.mil/

Federal Enterprise Architecture Models



SECTION 3 INFORMATION TECHNOLOGY

The **Corps of Engineers Enterprise Infrastructure Services (CEEIS) Program** provides management and services for the Corps network. More information is available in this document in the CEEIS Charges section. The CEEIS program's products and services are listed at https://www.ceeis.usace.army.mil/.

Utilization of the combination of the latest **Microsoft Windows Server Operating System and Active Directory (AD)** offers powerful technology that facilitates centralized security and directory management. USACE will utilize the features of administration delegation and assignment responsibility for Active Directory to execute a centralized management approach, but still allow for organizations to control administrative functions commensurate with their level. The minimum operational level requirements that Windows/AD must provide are:

Support interoperability
Policy and role based access
Directory services
Provide LAN services (user authentication, print to LAN printers, file storage on LAN file servers)
Facilitate reducing Total Cost of Ownership (TCO)
Support Server Consolidation
Facilitate reduction in total number of servers
Strict adherence to The Army's AD Naming Convention and Schema
Physical security and administrative control of AD Domain Controller

Corps IT organizations should continue following guidance previously given on preparation for migration from the Windows NT environment. The migration from the Windows NT environment to the Windows 2000/2003 environment is mostly a technology refresh. The PMP for migration to the latest Microsoft Windows Server operating system and Active Directory was released during Q1 FY 04.

Regionalizing IT Office Automation and Infrastructure Services. Since these services are a large percentage of the USACE IT portfolio, FY 04 is a time of planning for increased regionalization of IT office automation and infrastructure services. New business models for the provisioning of regionalized baseline services must be evaluated. Suggested categories for evaluation include helpdesk management; configuration architecture and engineering; deployment management; software distribution management; asset management; license management; hardware repair; and, install/move/add/change functions.

There are several factors that influence this guidance. Specifically, goals of USACE 2012 are to achieve greater organizational efficiencies through regionalization and nationalization of IT services. The USACE Competitive Sourcing Plan, Fair Act Inventory, recent Command-wide Functional Area Analyses (FAAs), and Office of Management and Budget (OMB) direction to develop an agency-wide business case for increased IT efficiencies necessitate formal planning during FY 04.

Expect guidance on what is to be included in the Command's definition of baseline services during first quarter FY 04, along with guidance on developing Service Level Agreements (SLAs). Major Subordinate Commands, Centers, ERDC, and separate Field Operating Activities' plans for regionalizing IT office automation and infrastructure services are due back to the USACE Chief Information Officer (CIO) by third quarter, FY 04. Each region must plan and strive for a minimum 10% reduction of these costs each year through 2008. The goal is to begin executing these plans in FY 05.

The Civil Works Program FY 04 Budget Passback reduced the Command's Civil Works IT Investment Portfolio from $315M to $299M for IT investments across *all* business and organizational levels. One of the largest categories of FY 04 planned IT investments is "Office Automation." The expectation is that during FY 04/FY 05 the Command will move to significantly reduce costs and contracts in IT office automation and infrastructure services in keeping with the FAA performance goals mentioned earlier in this section. At the time of IT Portfolio submission to OMB, the following were some of the larger Civil Works Program Office Automation (hardware and software) budget projections:

Organization	FY 04 Projected OA Investments
MVD	11.2M
NAD	11.0M
SAD	10.4M
NWD	9.0M
LRD	7.0M
SWD	7.0M
ERDC	6.0M
POD	4.0M
SPD	3.4M
HQUSACE	1.3M
HNC	1.0M
	(source ITIPS)

GOAL 2: Technology Insertion. Implement emerging information technologies to achieve breakthrough performance for USACE customers, partners, stakeholders, and citizens.

Key Outcome Measures: Increases in web-enabled applications and legacy system conversions; increased bandwidth to the desktop; growth in the use of collaborative technologies and knowledge sharing; leveraging enterprise level IT contracts.

USACE "Oracle Store." Oracle products and price lists available for Corps-wide use are described at https://corpsinfo.usace.army.mil/ci/liaison/oracle/index.html

The Directorate of Corporate Information and CEEIS joined with other Army MACOMS to negotiate an initial 50% discount over the standard GSA cost for ORACLE products through the CECOM BPA. This contract also provides full functionality of Oracle software licenses, direct support access to ORACLE Metalink and basically one-stop shopping for all ORACLE products. As participation in this new contract increases, additional discount savings will be evaluated and passed on to all customers.

Funding for Oracle software license purchases and maintenance depends on the number of licenses currently owned by the Activity. At the beginning of the fiscal year each customer or office will be required to establish a Government Order (GO) to cover annual maintenance cost. The GO will be issued and automatically accepted without prior forwarding to ERDC for acceptance. For new purchases, a GO should be prepared by the ordering activity for cost of purchased licenses and prorated yearly maintenance. Spreadsheets detailing CEFMS Government Order number and billed amounts for each activity will be sent to USACE Finance Center for billing and collection. Third quarter notification of proposed next FY annual maintenance costs will be sent to license holders. (Ordering information and document tracking is done by the CEEIS Asset Management Group.)

USACE IT Services Blanket Purchase Agreement (BPA). BPA #GS10TR-01-BNA-0026 was awarded 14 April 2002 and is available for Corps-wide use. A wide range of IT support services are described at http://www.usace.army.mil/ci/itacq/contract.html This BPA provides a minimum 10% discount over published GSA pricing schedules.

Other opportunities for technology insertion can be found at the web sites below. (This is not meant to be an inclusive list.)

Corporate Information Technology (IT) Acquisitions Home Page.
http://www.usace.army.mil/ci/itacq/itacq.htm

SECTION 3 INFORMATION TECHNOLOGY

Information Technology Laboratory
http://tsc.wes.army.mil/esribpa/

Army Contracts/Blanket Purchase Agreements
http://pmscp.monmouth.army.mil/contracts/contracts.asp

U.S. General Services Administration
http://www.gsa.gov/Portal/buying.jsp

Federal Business Opportunities
http://www.fedbizopps.gov/

Commands are encouraged to use these contracts to take advantage of negotiated savings.

Performance-Based Services Acquisition (PBSA). It is the policy of federal government, including DoD components, to implement performance based methodologies into services acquisition, including IT services. To the maximum extent practicable, the Corps shall use performance-based methods for acquiring IT services. To be considered performance-based, an acquisition should contain, at a minimum, the following elements:

- Performance Work Statement. This describes the requirements in terms of measurable outcomes rather than by means of prescriptive methods.
- Measurable Performance Standards. To determine whether performance outcomes have been met, these define what is considered acceptable performance.
- Remedies. Procedures that address how to manage performance that did/does not meet performance standards. While not mandatory, incentives may be used where appropriate.
- Performance Assessment Plan. Describes how contractor performance will be measured and assessed against performance standards.

More information is available from the DoD Performance Based Acquisition Guidebook available at https://corpsinfo.usace.army.mil/ci/liaison/pbsaguide010201.pdf

Goal 3: Information Assurance. Provide a high assurance of confidentiality, integrity, and availability of Corps IT assets.

Key Outcome Measures: IA is an integral component of a system's life cycle processes, from concept development through retirement; is an aggressive IA Awareness Program; adopts

Smart Card technology to improve identity management; reduces the quantity of incidents and mitigates the impact of break-ins; ensures Federal Information Security Management Act (FISMA) compliance.

Identity Management. Regional and District CIOs will be required to pay particular attention to the Department of Defense (DoD) requirement to implement Common Access Cards (CAC) and Public Key Infrastructure (PKI), as these are the cornerstones of a DoD wide effort to embrace identity management. In this context:

- The CAC will replace the current series of paper Standard Identification Cards.
- The CAC will be also preferred as the primary access card for facilities and controlled spaces.
- PKI will provide the basis of a cryptographic infrastructure that supports key, privilege and certificate management, and will enable positive identification of individuals using network resources.

This new asymmetric key process will replace the symmetric key CEFMS card processes used today.

DoD CAC/PKI implementation plans are available from CIO/G6 websites. Shortcomings in these efforts are well known, and mitigation efforts will be required. Sustainment of CAC/PKI will impose new burdens at the local level for:

- CAC PIN Reset,
- Certificate Maintenance,
- CAC Re-issuance, and
- Certificate Escrow.

At the CEEIS Program level, in coordination with local offices, new procedures will be required for capturing and "publishing" certificates to appropriate venues, and receiving and distributing Certificate Revocation Lists (CRLs) from Defense Information Systems Agency (DISA). Implementation requirements for these issues are neither resourced by dollars and FTE's, nor fully understood at this time. The DoD PKI effort is very much an evolutionary program which is essential to the long term security efforts of DoD.

SIPRNet. The classified SECRET Internet Protocol Router Network (SIPRNet) typically supports Combatant Commands, intelligence-related activities, war-room planning, deployment, transportation, and emergency operations activities. In the post 9/11 environment, this includes Homeland Defense efforts in which the Corps participates. To ensure an enterprise capability to support the nation in war as well as peace, Regional Level and District Level Commands

are required to provide the necessary facilities (secure room) to house a RED LAN. Commands that are not funded by DCSOPS must fund their requirements, which includes non recurring cost (NRC) and monthly recurring cost (MRC) for secure (encrypted) connectivity, secure devices, AISs, operating systems, applications, accessories and associated devices, hardware and software (IT). Commands will also provide funding for operating and maintaining systems administration. The CECI Directorate will provide project\program management and Connection Approval Process (CAP) guidance and support. Commands are required to complete security certification and accreditation documentation and submit to CECI-A for review and submission to NETCOM and NS52. Commands must also understand that this is parallel with other efforts to be completed for connectivity. There are other major efforts Commands must be concerned with to obtain direct SIPRNet connectivity, such as, Initial Modeling Request; If Contractor or Non-DOD – Validation; Security Accreditation Documentation, Secure Facilities.

IAVA. A critical piece of the overall information security posture is compliance with all Information Assurance Vulnerability Alert (IAVA) required actions. IAVA compliance must be acknowledged and reported on in The Army Compliance Reporting Database (CRD). Failure to address IAVAs promptly puts enterprise resources and connected resources at risk, and under AR 25-2 will result in punitive actions.

Training. All IA personnel are required to register, and to maintain a current status of their training. All enterprise and workstation assets must be reported and maintained. Mandatory DoD and DA IA training is documented at https://corpsinfo.usace.army.mil/ci/ia/training.html. All locations will complete all mandatory training, and maintain all IA personnel at certification level II. Recertification will be accomplished on an annual basis, by either attending an IA workshop or, if travel funds are short, by completing one of the IA Educational CDs at https://corpsinfo.usace.army.mil/ci/ia/cdtrain.html
Divisions, Centers, Labs, Districts and FOAs send Systems Administrators (SA) working on Windows 2000 Servers to the DA SA course for Windows 2000 security. DA will pay for tuition; units must fund for TDY and travel.

DITSCAP. In the current information technical environment, we must implement security on multiple tiers inside our organization with the cooperation of the whole team and must document this process for external review. As a DoD component, we must comply with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Specific information may be found at https://iase.disa.mil/ditscap/DitscapFrame.html. An automated tool has been purchased by CECI, which is helpful in completing the DITSCAP documentation. For more information see https://corpsinfo.usace.army.mil/ci/ia/training.html

Divisions/Districts must have valid accreditation packages on LAN, local AISs, and systems maintained. The Designated Approving Authority (DAA), the organizational Commander, will approve accreditation requests. (See Letter of Delegation of Authority https://corpsinfo.usace.army.mil/ci/ia/ditscap.html) At a minimum, each site must have an Interim Authority to Operate (IATO). Currently less than 22% of the Corps information infrastructure is properly accredited. Of the AISs in the corporate inventory, only 8 have an Authority to Operate (ATO), and only an additional 5 have an IATO.

Commanders are reminded that security accreditation procedures apply to Supervisory Control and Data Acquisition (SCADA) Systems, as well as to LANs and WANs. Although not traditional business systems, SCADA systems are information systems and must be accredited using the DITSCAP, either individually or as part of a larger system. The DITSCAP process allows local commanders to be aware of the risks for which they are responsible.

Corps of Engineers Enterprise Infrastructure Services (CEEIS) must have a valid accreditation package on the WAN, to include the two processing centers, and the systems they maintain (i.e., UPASS). The USACE CIO is the DAA and will approve CEEIS accreditation. Corps-wide, AIS Functional Proponents must submit accreditation packages for the systems being developed/maintained such as CEFMS to the USACE CIO, as the USACE DAA, for approval.

COOP. Because we rely on our information systems and data communication networks in the performance of critical civil and military missions, continuity of operations under difficult circumstances is essential. The CEEIS Program Management Office is working on an overall enterprise Continuity of Operations Plan (COOP), including COOP capabilities required for corporate systems that run within the CEEIS production environment. A nucleus of COOP capabilities required by corporate systems must be available in FY 04.

IDS. CEEIS is responsible for the network based Intrusion Detection Systems (IDS) that are required at all entrances and/or gateways to the CEEIS wide area and local area communications networks. CEEIS will verify that each corporate gateway has an IDS, and will also maintain and monitor all corporate firewalls and IDS devices. (Local sites may have the ability to read these mandatory devices where the software supports read only access). CEEIS will install IDS on critical processing center servers, and will monitor mandatory IDS devices.

Army Policy requires host-based Intrusion Detection Systems, IDS, on Information Assurance Servers that support dial-in systems (RADIUS compliant server), and on all mission critical systems. (A server is critical if the loss of the server will severely impact the command's ability to perform its mission).

Corps sites (Divisions, Centers, Labs, Districts, and FOAs) will ensure all outside connections (non-Corps connections) at their site have IDS. Divisions, Centers, Labs, Districts and FOAs will add host-based IDS to mission critical servers including dial-in servers. Functional proponents will install IDS on all critical servers for applications, including web-based or enabled, not hosted at the CEEIS processing centers. CEEIS will monitor the IDS information for these connections. Where possible, this information will also be provided to the sites.

Virtual Private Networks. Virtual Private Networks (VPNs) are an evolving component of the Corps' overall security architecture. CEEIS will provide a VPN infrastructure in support of external access, including telework and contract support activities.

Federal Information Security Management Act (FISMA). The Corps is currently beset by a host of "new" reporting requirements. Actually, these have been around for a while in form but not in practice. The FISMA, which replaced the Government Information Security Reporting Act (GISRA), treats security as a continuum – from the "real" physical world to the cyber world – and requires that all aspects of security be addressed, and reported. Because of USACE "dual" mission status, this burden falls upon the Corps more rigorously than it does on the rest of DoD. Expect a high level of attention for FISMA compliance to continue for the foreseeable future.

There are no easy solutions for total information system security. We must implement security on multiple tiers inside our organization with the cooperation of the whole corporate team. Proponents for civil and military missions must determine security risks and implement critical system security devices and practices. For up-to-date information on AIS security issues, see https://corpsinfo.usace.army.mil/ci/ia/

GOAL 4: IT Investment Management. Maximize business value and manage risk associated with USACE IT investments using the Capital Planning and Investment Control (CPIC) Process. A description of the CPIC Process is available at https://corpsinfo.usace.army.mil/ci/cfat/.index.html

Key Outcome Measures: Selecting IT projects with the best business value; improving the Capital Planning and Investment Control (CPIC) Process; risk mitigation in Project Management; and migration of individual IT projects into programmatic management processes to fulfill USACE business goals.

The CPIC evolved significantly for evaluation and prioritization of FY 04 and FY 05 corporate IT investments. Improvements included expanding the Cross Functional Assessment Team (CFAT) membership to all field organizations; the CFAT's use of additional evaluation criteria

over previous years ; establishment of an Executive Functional Assessment Team to validate output of the CFAT; integration of process output; *i.e., authority levels*, with Appropriation Managers in CERM, CECW, and CEMP for both execution and planned budget requirements. Output of the CPIC Process resulted in approximately $12M cost avoidance for FY 04 corporate IT requirements. Results of the CPIC Process can be viewed at https://corpsinfo.usace.army.mil/ci/cfat/MFRENCL3.xls.

The CPIC Process will continue to evolve using the input from the CFAT's After Action Report of the past cycle. A Process Development Team (PDT) was established in the 4th Qtr, FY 03 to further evolve the process. The current EC 25-1-303, Information Technology Investment Management is undergoing revision to reflect the changes to the process.

All USACE MSCs, Districts, Labs, Centers, FOAs are required to have a CPIC Process in place to review, evaluate and prioritize IT investments per paragraph 10, of EC 25-1-303. This is subject to review under Command Staff Inspections.

Corps IT Investment Business Cases (Exhibit 300). Eleven business cases were presented to OMB as major investments in the FY 04 IT Portfolio. During FY 04, the CIO will be working with functional proponents to evaluate how well these investments have met declared performance goals and measures. Updated information on key life cycle actions related to corporate IT systems and programs are found at https://corpsinfo.usace.army.mil/ci/liaison/liaisonais.html

GOAL 5: E-Government. Refine web-based electronic information access and delivery for sharing, creating single points of access, reducing reporting burdens, eliminating paperwork by changing to electronic systems, and streamlining business transactions.

Key Outcome Measures: Align Command with the President's e-Government Management Agenda (PMA); compliance with the e-Government Act of 2002; increased emphasis on electronic records management.

Command PMA Participation. In FY 04 the Corps of Engineers is expected to continue its participation in several of the interagency PMA initiatives, contributing both resources and "in-kind" FTE. As the Command analyzes its IT Investment Portfolio, it is also expected to demonstrate leadership *at all organizational levels* in seeking interagency opportunities to partner on IT projects. Before an IT investment is made, an e-government review will be conducted to see if there are opportunities for both using e-business technologies and collaboration across organizations and agencies. More information about the PMA is available at http://www.results.gov/index.html

The following are samples of the Corps PMA-level participation:

PMA-Level Initiative	FY 03	FY 04	FY 05
Government to Citizen (G2C)			
Recreation One Stop. FY 04 will include the National Recreation Reservation System (NRRS), as well as portal support.	$ 50K	$ 5.4M	$ 5.45 M
Government to Business (G2B)			
Online Rulemaking. The Corps public regulatory dockets (Federal Register) will be made electronically accessible through Online Rulemaking.		$ TBD	$ TBD
Federal Asset Sales Goal is to establish on-line auction/sales portal. Corps has delegated property disposal authority for Civil Works Program. However, most actions are accomplished through GSA.		$ TBD	$ TBD
Government to Government (G2G)			
Geospatial One Stop. Portal support and FTE in-kind service for Marine Transport standards development. Over 4500 meta files posted to NSDI node from 28 Districts.	$ 100K 5.5 FTE	$100K 5.5 FTE	$ 100K 5.5 FTE
Disaster Management . Corps is managing partner with GSA for interagency Exhibit 300 business case, based on ENGLink-I. Plans to contribute agency content to portal.		$ TBD	$ TBD
Internal Efficiency and Effectiveness(IEE)			
Integrated Acquisition Processes. Corps is participating in migration to Wage Determinations On-line (WDOL.gov).		$ TBD	$ TBD
Cross Cutting			
E-Authentication. CEFMS e-signature capability and P2 single sign on has visibility in OMB surveys.			
Volunteer.Gov. in partnership with the White House's USA FreedomCorps Network.	$ 12.5K	$ 12.5K	$ 12.5K

Federal Records Management (RM) Requirements. These requirements provide for cost-efficient and systematic life cycle management of all recorded information, regardless of media and format. Continuing RM programs capture, preserve, and make available evidence essential for USACE decisions and actions, preserve permanently valuable information, protect the rights and interests of USACE, soldiers, citizens, and the Government, and meet the needs of the American public. Commanders at all echelons are required to document USACE official business and ensure accessibility of information throughout its life cycle. Regional level and District CIOs should be implementing the new Army Records Information Management System (ARIMS) as prescribed under revised AR 25-400-2 and enforcing the standards set forth. Records management functions should be integrated into all automated information systems (AIS). Electronic recordkeeping systems compliance with ARIMS, USACE-wide Electronic Document Management System (EDMS) Guidelines and Standards, and DoD 5015.2-STD, Design Criteria for Records Management Applications should also be ensured. Information concerning these matters can be found at http://www.usace.army.mil/ci/recmgmt.

Ensuring Quality Information is Disseminated to the Public. In accordance with OMB Information Quality Guidelines (IQG) requirements, a basic standard of quality (objectivity, utility, and integrity) must be maintained and appropriate steps taken to incorporate information quality criteria into USACE public information dissemination practices. Particular emphasis is placed on scientific, environmental, financial and statistical information produced by an agency. By FY 04, USACE-wide IQG program responsibilities will be assigned, a web-based administrative mechanism will be put in place for the public to seek and obtain correction of disseminated information, and annual reporting requirements will be issued.

Web Policy. As the Corps becomes more dependent on the World Wide Web for communication with customers and partners, ensuring that best business and IT practices and policies are followed becomes more important. Commands are reminded that recently issued policy on personally identifying information and compliance with Section 508 of the Rehabilitation Act are continuing responsibilities.

All Corps Website Managers, Webmasters, and Pagemasters should join both the Corps Webmasters List (CDL-Webmasters) and the DoD Webmasters mailing list for opportunities to stay informed about the latest policy information and discuss issues with colleagues. More information is available at http://www.dod.mil/webmasters/faq/index.html

Enterprise Portal. The *e*-Corps Portal, single sign on, and lessons learned capture capability will continue to be prototyped by the Chief Information Officer during the first part of FY 04, with results reported out to the various Headquarters/Command committees. Integral to the enterprise portal prototyping effort will be development of "views" to enhance delivery of agency products and information services. Three views will be focused on the public, stakeholders/business partners, and the internal Corps team. Use of Army Knowledge On-Line (AKO) and the building of enterprise content via AKO are encouraged. Functional areas are also encouraged to develop Communities of Practice (COP) within the electronic virtual teaming environment.

OTHER GUIDANCE

Strategic Sourcing. The Corps is working to comply with the President's Management Agenda and the Army's Third Wave competitive sourcing initiatives. These initiatives require all federal agencies to streamline and become more effective. "Competitive sourcing" means that all federal agencies are reviewing their tasks to determine if a given task is something that must be done by the federal government, or if it could be done by a civilian contractor and would be competed. The administration, management, and product/service delivery of information technology (IT) is not a "core" competency for the Corps; however, it is a critical competency with respect to meeting public law and regulatory management requirements and for improving the effectiveness, efficiency, and quality of USACE mission and program execution. Within USACE, IT is the umbrella for the functions, processes, activities and tasks associated with Information Resource Management (IRM), Information Assurance (IA), and the Information Mission Area (IMA). The IMA includes automation, communications, records management, visual information, printing and publication, and libraries. USACE, by public law, executive orders, directives, regulations and memoranda, must plan, acquire, operate, maintain, and manage its information resources (hardware, software, services, and training/maintenance support) and protect its data and information from unauthorized access, denial of service, and change/destruction. The product/service areas of IT are prime candidates for strategic competitive sourcing. Additional information on/about competitive sourcing can be found at http://www.hq.usace.army.mil/cepa/compsource/compsource.htm.

IT/IRM Work Force Development. All commands should encourage their Directors/Chiefs of Information Management to complete the Advanced Management Program or CIO Certification Program at the National Defense University's IRM College. Program information can be found at http://www.ndu.edu/irmc/.

The Federal CIO Council Human Capital and Workforce for IT Committee, in conjunction with the Office of Management and Budget, is also placing emphasis on qualifications and competencies of individuals serving as project managers (PM) for "major" IT projects. Qualified project managers are defined as possessing:

- Experience managing IT projects of similar size and scope, within 10% of the baseline cost, schedule and performance goals, or,
- A government project management certification, or a commercial certification, such as the Project Management Institute (PMI), and,
- Dedication to the IT project or program on a full-time basis.

For “major” IT projects within the Corps, these guidelines for selecting a PM should be taken into consideration at all organizational levels. A “major” IT project is defined as having significant importance to the organization, high executive visibility, major dollar investment, or be e-Government/e-business in nature.

Defense Communications System (DCS). The acquisition and project/program management for telecommunications networking technologies and information technologies supporting USACE infrastructure services to meet USACE Command, Warfighter and critical mission requirements includes the DCS, which is a composite of certain Department of Defense (DOD) and MILDEPs, NS/EP, C4/I communications systems and networks (netcentric). The information system provides, long haul, regional, point-to-point, satellite and switched network telecommunications circuits, systems and services for global communications. Long-haul telecommunications services comprise any and all voice, data, and video switching and transmission services and associated network management, satellite, wireless, asynchronous transfer mode (ATM) edge devices and regional services or metropolitan area networks (MANs). The Defense Information Systems Agency (DISA) and the Army CI0-G6/NETCOM provides centralized management and billing services for command, control, communications, computers, and intelligence, surveillance and recon (C4/ISR) systems of the DCS. Therefore, USACE Commanders must program budget for and develop plans to acquire, operate, and maintain DCS requirements appropriate for their missions. However, HQUSACE/CECI pay a consolidated bill for DCS on a quarterly basis for whatever products, support and services each command acquires. Consequently, each command must remit to HQUSACE (instructions by separate memorandum) the funds needed to pay this consolidated bill. Commands are to use their current cost as a baseline to estimate their FY 04-05-06 funding requirements for DCS services that are planned, acquired, and/or sustained. Each command must plan, program, and budget for their DCS requirements to be able to remit to HQUSACE the funds needed to pay for the services and support. Request for remittance of estimated payments for each fiscal year will be made in late March or early April. The following table estimates the consolidated bill for the DCS, long-haul communications technologies and supporting services. The CECI Directorate does not charge a fee for service for these services.

DCS	FY 03 Estimate	FY 04 Estimate	FY 05 Estimate	FY 06 Estimate
	2.1M	2.6M	2.8M	3.1M

Acronym List

AD	Active Directory
AKO	Army Knowledge On-Line
ARIMS	Army Records Information Management System
ATO	Authority to Operate
BPA	Blanket Purchase Agreement
C4ISR	Command, Control, Communications, Computers, Information, Surveillance & Reconnaissance
CAC	Common Access Card
CeA	Corps Enterprise Architecture
CECOM	Communications-Electronics Command
CEEIS	Corps of Engineers Enterprise Infrastructure Services
CFAT	Cross Functional Assessment Team
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
COP	Communities of Practice
CPIC	Capital Planning and Investment Control
CRD	Compliance Reporting Database
CRL	Certificate Revocation Lists
DAA	Designated Approving Authority
DCS	Defense Communications System
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
EDMS	Electronic Document Management System
EFAT	Executive Functional Assessment Team
FAA	Functional Area Assessment
FEAF	Federal Enterprise Architecture Framework
FISMA	Federal Information Security Management Act
GISRA	Government Information Security Reporting Act
GO	Government Order
IA	Information Assurance
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IQG	Information Quality Guidelines
IDS	Intrusion Detection Systems

SECTION 3 INFORMATION TECHNOLOGY

IRM	Information Resources Management
IT	Information Technology
IT/IM	Information Technology/Information Management
LAN	Local Area Network
MAN	Metropolitan Area Network
OMB	Office of Management and Budget
PBSA	Performance-Based Services Acquisition
PKI	Public Key Infrastructure
RM	Records Management
SA	Systems Administrators
SCADA	Supervisory Control and Data Acquisition
SIPRNet.	SECRET Internet Protocol Router Network
SLA	Service Level Agreements
TCO	Total Cost of Ownership
VPN	Virtual Private Networks

The POC is Sally Mahoney, 202-761-7135.